UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,889	12/07/2005	Junbiao Zhang	PU030227	2851

24498 7590 02/14/2011
Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
NGUYEN, TRONG H	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
02/14/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/559,889	**Applicant(s)** ZHANG ET AL.	
	Examiner TRONG NGUYEN	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-14* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 11/19/2010. In response to the office action mailed on 06/21/2010, claim 9 has been amended. Pending claims include **claims 1 and 3-14**.

The rejection of claim 9 under 35 USC 112, second paragraph has been withdrawn due to Applicant's amendment.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 8 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. **Claims 1 and 4** are objected to because of the following informalities:

Claim 1 line 13 and claim 4 line 4 recite "said access point" which should be "the access point" for consistency.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 7-8, and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan et al. US 2004/0081320 A1 (hereinafter "Jordan") in view of Chen et al. US 2003/0221098 A1 (hereinafter "Chen").

Regarding claim 1, Jordan discloses **a key synchronization method for a wireless network** [e.g. Figs. 1, 8-11] **comprising:**

setting a current encryption key and an old encryption key at a point in the wireless network; [e.g. pars. 0080-0081, 0083, 0084, 0089-0091, 0093: Jordan's key synchronization method starts out with an initial or base password key (let's call it K1) being a current password key (i.e. current password key is set to K1) at a messaging gateway and a wireless device. Later, when a new password key is generated (let's call it K2) at the messaging gateway, K1 becomes a prior or old password key (i.e. old password key is set to K1) and K2 replaces K1 to become the current password key (i.e. the current password key is set to K2). Both the messaging gateway and the wireless device use this same key K2 to securely communicate with one another]

generating a new encryption key at the point; [e.g. pars. 0078-0079, 0083: At some later point in time, another new password key is generated (let's called it K3) at the messaging gateway]

resetting at the point the current encryption key to equal the newly generated encryption key; [e.g. pars. 0081, 0083: K3 replaces K2 to become the current password key (i.e. the current password key is set to K3) at the messaging gateway]

resetting at the point the old encryption key to equal an encryption key being used by a station in communication with the point; [e.g. pars. 0080 and 0083: K2, a password key currently being used by a wireless device in communication with the messaging gateway, becomes the old password key (i.e. the old password key is set to K2)]

communicating the newly generated encryption key from the point directly to the station in an encrypted form using the old encryption key; [e.g. pars. 0078, 0080, 0082-0083: K3 is transmitted from the messaging gateway to the wireless device in an encrypted form using the old password key]

indicating at the point a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, [e.g. pars. 0087-0088, 0090: messaging gateway initiating a function that communicates to the wireless communication system that the updated password key is not correct or sending an error message to the wireless device or pars. 0091-0093: indicating a decryption failure by reverting back to a password key that is prior to the most recent updated password key] **wherein a data frame that failed to decrypt using the current encryption key is decrypted by said point using the old encryption key;** [e.g. pars. 0091-0093: messaging gateway reverting back to a password key that is prior to the most recent updated password key (i.e. the old password key)]

resetting at the point the old encryption key to equal the current encryption key when decryption using the new encryption key is successful [e.g. pars. 0088, 0091, 0078, 0083: when the messaging gateway and the wireless device are re-synchronized (i.e. both contain most recent updated password key or K3), another new password key (let's called it K4) can be generated which results in K3 becoming the old password key (i.e. the old password key is set to K3)]

Although Jordan discloses that the above steps: setting, generating, resetting, resetting, communicating, indicating, decrypting, and resetting are performed at a point in the network (i.e. messaging gateway), Jordan does not specifically disclose that the above steps: setting, generating, resetting, resetting, communicating, indicating, decrypting, and resetting are performed at **an access point** and that the newly generated encryption key is communicated **directly** from the **access point** to the station.

However, Jordan discloses that the above wireless communication system shown in Fig. 1 is an exemplary embodiment of a wireless communication system in which Jordan's synchronization methods may be implemented (pars. 0033-0034). Thus, one of ordinary skill in the art would readily recognize that Jordan's synchronization methods can be implemented in other wireless communication systems where there is a need to maintain secure wireless transmissions including a wireless communication system comprising access points and stations.

Furthermore, Chen discloses a method for updating and synchronizing ciphering key between at least one access point in direct communication with at least one station in a wireless network to prevent network hackers from invading into the wireless network where a newly generated encryption key is transmitted directly from the at least one access point to the at least one station in encrypted form using an old encryption key (e.g. Fig. 2 and pars. 0005, 0012, 0043).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan by implementing the above synchronization method in a wireless communication system comprising at least one access point in direct communication with at least one station and communicating the newly generated encryption key directly from the at least one access point to the at least one station as described by Chen for the purpose of preventing hackers from invading into the wireless network (Chen, pars. 0005, 0012).

Regarding claim 7, Jordan-Chen combination further discloses **the method according to claim 1**, **wherein said setting is performed by the access point for each station in the wireless network** [see rejection of claim 1 and Chen's Fig. 2 and par. 0017]

Regarding claim 8, this claim is rejected for similar reasons as in claim 1.

Regarding claim 13, Jordan-Chen combination further discloses **the method according to claim 1**, **wherein the new encryption key is generated at the access point upon expiration of a key refresh interval** [e.g. Chen, par. 0054: As long as the random-code generation program 38 is detonated to generate a new ciphering key each time the counting module 36 conforms to a predetermined time, it is covered by the disclosure of the present invention. In addition, the predetermined time can be a fixed time or a non-fixed time. That means the wireless network system 30 can update the common ciphering key according to a fixed time or a random time. No matter if the common ciphering key is updated according to a fixed time or a random time, the ciphering key also can be automatically updated]

6. **Claims 3, 4, 9 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan in view of Chen and further in view of Loc et al. US 7,293,289 (hereinafter "Loc").

Regarding **claim 3**, Jordan-Chen combination further discloses **the method according to claim 1, further comprising: decrypting received data frames at the access point using the old encryption key** as [see rejection to claim **1** above] but does not specifically disclose the received data frames are **associated with said out-of-sync counter** and **incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key**.

However, Loc discloses a method for detecting a security breach in a network wherein “Each time a client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented” (Fig. 5, Col. 6, lines 59-61). Furthermore, Jordan discloses that when there is a transmit or receive error, the messaging gateway reverts back to a password key that is prior to the most recent updated password key (i.e. the old encryption key) to decrypt a message received from the wireless device after unsuccessfully decrypting the message using the updated password key (i.e. the current password key) (Figs. 10-11).

Loc, Chen, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key and decrypting received data frames associated with said out-of-sync counter as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23) and resynchronizing password keys (Jordan, Par. 0087).

Regarding <u>claim 4</u>, Jordan-Chen combination further discloses **the method according to claim 1, further comprising:**

decrypting, using the new encryption key, the received data frame from the station when the access point determines the station sending the received data frame is using the new encryption key, said access point starting to use the new encryption key when a first data frame correctly encrypted with the new encryption key is received from the station; [e.g. Jordan, Figs. 10-11, Pars. 0088-

0089 and 0091-0092 and Chen, par. 0051] but does not specifically disclose **re-setting an out-of-sync counter to zero upon successful decryption**.

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 successfully decrypts a packet, the encryption failure counter is reset to zero" (Loc, Col. 6, lines 57-69).

Loc, Chen, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by re-setting an out-of-sync counter to zero upon successful decryption as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding <u>claim 9</u>, this claim is rejected for similar reasons as in claim 3.

Regarding <u>claim 14</u>, Jordan-Chen-Loc combination further discloses **the method according to claim 3, wherein said out-of-sync counter comprises a predetermined threshold that if exceeded causes communication to terminate between the access point and a source of the data frames causing the threshold of said out-of-sync counter to be exceeded** [Loc, Col. 6, lines 61-65: When the encryption failure counter reaches a predetermined threshold n (that is, when n consecutive failures have occurred) (step 512), client 108 sends an alert packet to access point. Loc, Col. 6, lines 5-9: furthermore, upon receiving the alert of a security breach, the access point "responds by immediately removing the MAC address of client 108 from its list of authorized clients, by ceasing to send any packets to the MAC address of client 108, and by discarding all packets that are received from the MAC address of client 108]

7. **Claims 5-6 and 10-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan in view of Chen and further in view of Kelem et al. US 6,118,869 (hereinafter "Kelem").

Regarding <u>claim 5</u>, Jordan-Chen combination discloses **the method according to claim 1** but does not specifically disclose **further comprising setting the old encryption key equal to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by setting the old key equal to a null value, said null value representing a no encryption mode as described by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding **claim 6**, Jordan-Chen combination discloses **the method according to claim 1** but does not specifically disclose **further comprising setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode as taught by Kelem in order to modify the keys to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding **claim 10**, Jordan-Chen combination discloses **the key synchronization system according to claim 8** but does not specifically disclose

wherein said at least one access point is configured for setting the old encryption key to a null value, said null value representing a no encryption mode.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by setting the old encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding <u>claim 11</u>, Jordan-Chen combination discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point is configured for setting the new encryption key to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by setting the new encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding <u>claim 12</u>, Jordan-Chen combination discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point initially sets the old encryption key to a null value**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jordan-Chen by setting the old encryption key at the access point initially to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Conclusion

8. Examiner cites particular pages or columns or paragraphs and/or line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, applicant fully considers the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 9:00 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T N/
Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436